

SECURITY PRIORITIES CHECKLIST



CRITICAL SECURITY (REQUIRED)

Required for EVERYONE.

☐ Do a Personal Password Audit

- ☐ Are the passwords for sensitive accounts unique?
- ☐ Are my passwords long instead of elaborate?
- ☐ Would my family have access (or know how to get access) to my accounts in case of an emergency?
- ☐ Should I use password managers? (recommended: [1Password](#))

☐ Set up 2FA on All Critical Accounts

- ☐ Prioritize investment, crypto and social media accounts;
- ☐ Install a mobile authenticator app (i.e. Google Authenticator) or purchase a 2FA security key (recommended: [Yubikey](#))

TIP: Learn how to set up 2FA using [this YouTube playlist](#).

☐ Change Your Home WiFi Router Password

- ☐ Consider creating a separate guest network so you don't have to give out your personal WiFi password

☐ Lock Your Devices (phone, tablet, computer) with a Passcode

- ☐ Set up "Find My Phone" or similar tracking

☐ Make ALL Social Media Private

- ☐ Facebook: Change [these 7 privacy settings](#)
- ☐ LinkedIn: Don't use your personal email as email contact (see [how to use email aliases](#))
- ☐ Instagram: Turn your account to "private"

**some links may be affiliate links*

HELPFUL SECURITY (RECOMMENDED)

Recommended based on your geographic location and situation.

☐ Freeze Your Credit

- ☐ Ask all major CRAs (credit reporting agency) to create a freeze

— Learn more about [how to set up a credit freeze](#).

☐ Monitor Your Identity & Credit

- ☐ Request credit report at least twice a year (calendar reminder)
- ☐ OR...pay for identity / credit monitoring (i.e. [Identity Force](#))

— Paying for monitoring isn't necessary unless you have already been hacked or you suspect you're being targeted.

☐ Reconcile Your Bank Account(s) Every Month

☐ Set a Government Records Alert for Your Name

— Learn how this can help [prevent home title fraud](#)

☐ Protect Your Personal Data Online

- ☐ Scrub your data online (or use a service like [DeleteMe](#))
- ☐ Consider a virtual address (recommended: [PostScan Mail](#))
- ☐ Consider a virtual phone number (recommended: [Hushed](#))

☐ Use a Separate Encrypted Email Account

- ☐ Create a free account (recommended: [ProtonMail](#))
- ☐ Change all banking and investment accounts to the private email address

☐ Use Privacy-Focused Internet Browser (anything BUT Chrome!)

☐ Set up an Email Masking service

- ☐ Sign up for email masking (recommended: [SimpleLogin](#), which is included with all [paid Proton Mail plans](#))
- ☐ Integrate with your password manager (such as [1Password](#))

OPTIONAL SECURITY MEASURES

Advanced Security Not Required for Most People

- ❑ **Use a Virtual Private Network (VPN)** - Recommend [NordVPN](#)
 - ❑ TIP: Set up the VPN on WiFi router for all devices
 - Useful for those who want to hide their IP address online to hide their internet activity. TOR is also an option, but it's slower.
- ❑ **Download Antivirus/Anti-malware Software**
 - Useful for those whose data has already been hacked and constantly receive phishing and malware attacks.
- ❑ **Move to Encrypted Cloud Backup** (recommended: Proton Drive)
- ❑ **Migrate to End-to-End (E2E) Encrypted Messaging Apps**
 - ❑ Download Signal and use instead of iMessage/WhatsApp
 - Using E2E messaging requires that you convince all your friends and family to do the same.
- ❑ **Move to Anonymous or Secured SIM card**
 - ❑ USA: Switch to [Efani](#) (uses AT&T network)
 - ❑ International: Switch to [Silent Link](#) (with anonymous payment)
 - Securing your SIM is useful for those who protect their crypto investments with SMS 2FA or who don't want their phone data to be trackable.
- ❑ **Switch to an Anonymous Search Engine**
 - ❑ Change my default search engine away from Google
 - ❑ OR...download the [StartPage Browser Extension](#) (free)
- ❑ **Set Up a Burner Credit Card Account**
 - ❑ USA: Open an account with [Privacy.com](#)
 - ❑ International (not all countries): [Revolut](#)

*some links may be affiliate links